Pudsey Waterloo Primary School
General Data Protection Regulation
Acceptable Use of ICT Policy

Introduction

Pudsey Waterloo Primary School commits to protecting the privacy and security of the personal information it holds for staff, pupils, governors, volunteers, and other individuals who engage with the school. Please note our Privacy Statements.

To complement the data protection duties of the school there are duties shared by all staff, governors and volunteers because, as a professional organisation with responsibility for children's safeguarding, it is essential that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This policy should be read in conjunction with:

- Pudsey Waterloo Primary School's Safeguarding and Child Protection Policy
- Owlcotes Multi-Academy Trust Data Protection Policy

Monitoring

Pudsey Waterloo Primary School has appropriate filters and monitoring in place as part of our obligation to comply with Keeping Children Safe in Education and the Prevent duty.

Internet filtering and monitoring arrangements are monitored at least annually to ensure that they continue to be appropriate, fit for purpose and safeguard the welfare of children by blocking harmful or inappropriate content without unreasonably impacting on teaching and learning.

Pudsey Waterloo Primary School requires all users of the internet network to access the network using their school supplied login credentials, with the exception of external visitors to school who are able to access the internet network using 'guest' login credentials. These measures are in place to monitor online activity and identify individuals if required. A safeguarding reporting system is in place for the SLT and DSL to monitor online activity and identify areas of concern if required.

This agreement covers all digital and physical data systems, e.g., the internet, intranet, network resources, learning platform, software, communications tools (online and offline), equipment (access devices) and paper records, whether printed or handwritten and however stored.

1. I understand that data held by the school may only be processed (acquired, processed, stored, deleted or transmitted) on the legal bases that the school has registered with the Information Commissioner's Office.
2. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the General Data Protection Regulation 2018. This means that all personal data will be processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely. Any data which is being removed from the school will be encrypted either on a school laptop, throughout suitable online storage e.g. Microsoft or on an encrypted storage device. Any images or videos of pupils will always take into account parental consent. I will ensure that data no longer needed will be effectively deleted or shredded.
3. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation. Such misuse is also covered by the GDPR and any such misuse must be reported to the ICO, and to the data subjects (people) affected, within 72 hours.
4. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my device as appropriate. I will not use personal equipment to access school data.
5. I will respect system security and I will not disclose any password or security information. I will use a 'strong' password. I will adopt school procedures for the safe storage of my passwords and for acquiring new ones.
6. I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones). Where possible I will use the School's network server to upload any work documents and files and, where appropriate, in a password protected environment. I will protect the devices in my care from unapproved access or theft. I will not share any files or folders on the school network with any other user outside the school or trust without the permission of the Headteacher. I will be mindful that when working in a public space that others may be able to see my laptop, tablet or mobile phone screen and will use my discretion as to whether information should be hidden from site. I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.
7. I will respect copyright and intellectual property rights.

8. I have read and understood the school's GDPR Policy and e-Safety Policy which cover the security of data and safe and appropriate access to data.
9. I will report all incidents of concern regarding children's online safety to the Designated Child Safeguarding Lead and/or the e-Safety lead as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable/extreme websites to the e-Safety Lead.
10. I will not attempt to bypass or alter any filtering and/or security systems put in place by the school.
11. My communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. All letters will be copied to the school office or if they are about a sensitive issue then the Headteacher. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.
12. I will refrain from using any form of social media to discuss any aspect of school life except purely social events that involve colleagues. I will follow any guidance issued when contributing to the use of social media by the school as an official communication channel.
13. My use of ICT and information systems and my written communication will always be compatible with my professional role whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites or postal addresses. My use of ICT and other forms of communication will not interfere with my work duties and will be in accordance with school policy and the law.
14. The school needs to implement technical and procedural controls to protect its ICT facilities as well as the data and well-being of its staff and students. These protective measures must not be disabled, bypassed, circumvented, or reconfigured. You must not prevent the timely installation or re-configuration of security controls. These protective measures include multi-factor authentication which may require, by the user, the installation of an application or receipt of a message on a personal device (typically a mobile phone) to confirm the user's identity when accessing ICT facilities. In instances where multi-factor authentication is required to confirm the user's identity, use of a personal device is permitted in school in order to facilities access.
15. I will not create, transmit, display, write, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role or the school into disrepute.
16. I will promote e-Safety (including privacy) with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create. Similarly I will promote care for others in the pupils' writing and any other content that they create.
17. I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.
18. The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or

unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I _____ (please print name) acknowledge that I have received and read and understood a copy of the Pudsey Waterloo Acceptable Use Policy.

Signed _____

Dated _____

This Acceptable Use of IT Policy was adopted by Pudsey Waterloo Primary School on 30/11/2020

Chair of Governors – Mrs M Smith		
Signature:		
Frequency of review:	2 years	
To be reviewed and approved by:	PWPS Full Board	
Date of next review:	April 2027	

REVIEW RECORD

Date of review	Reason for review	Date of next review
06/02/2023	Addition of 'monitoring' section.	February 2025

Name:		Signature:	

on behalf of PWPS Full Board

Date of review	Reason for review	Date of next review
28/04/2025	Addition of item 14.	April 2027

Name:			

on behalf of PWPS Full Board

Date of review	Reason for review	Date of next review

Name:		Signature:	

on behalf of PWPS Full Board